Number: CSB-160407-1

Released: April 7, 2016

Modified:

Subject: FortiAnalyzer drops logs sent from FortiGate devices

Product: FortiAnalyzer

Description:

A FortiAnalyzer running 5.2.6 may stop receiving logs from all devices if all the following conditions are met:

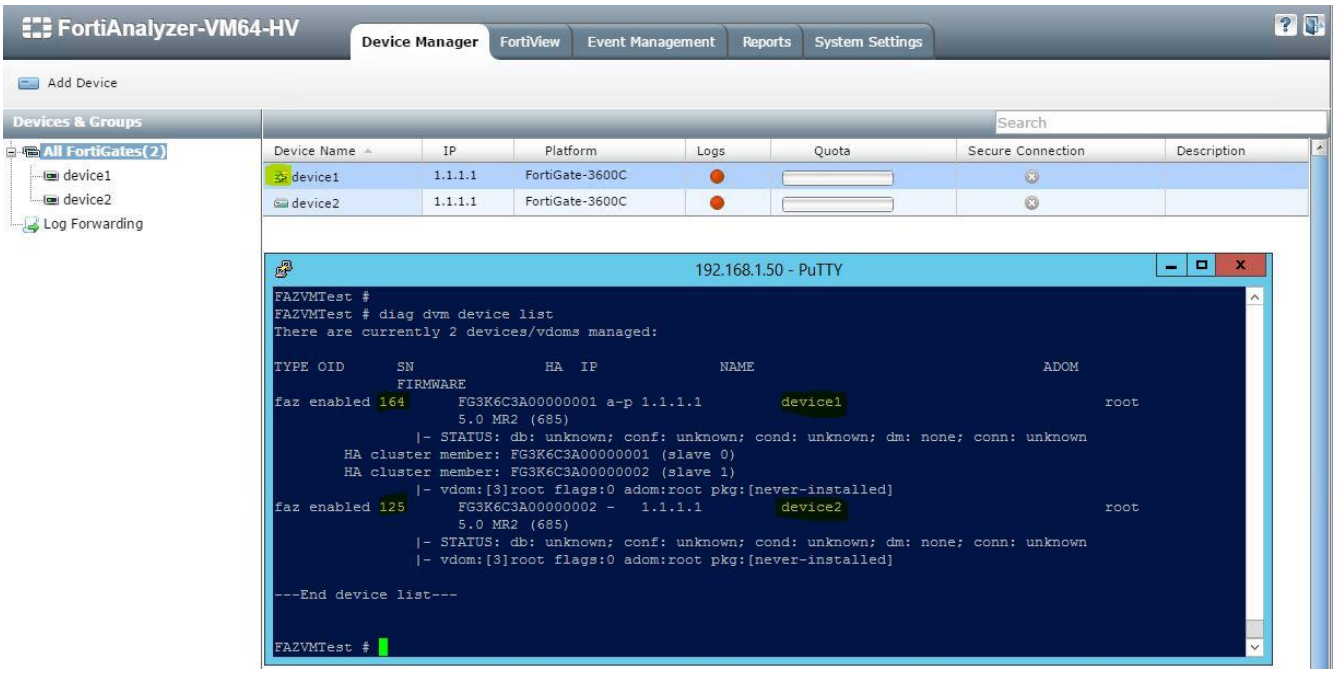
(1) FortiGate devices are registered as an HA cluster before or after the upgrade to 5.2.6.
(2) After the HA cluster registration, the slave device has not been deleted.
(3) The slave device has a lower system generated object ID (OID) than the cluster OID.

To verify:

diag dvm device list

```
TYPE OID     SN              HA  IP          NAME                ADOM                FIRMWARE
faz enabled 164     FG3K6C3A00000001 a-p 1.1.1.1     device1     root                5.0 MR2 (685)
            |- STATUS: db: unknown; conf: unknown; cond: unknown; dm: none; conn: unknown
      HA cluster member: FG3K6C3A00000001 (slave 0)
      HA cluster member: FG3K6C3A00000002 (slave 1)
            |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
faz enabled 125     FG3K6C3A00000002 -   1.1.1.1     device2     root                5.0 MR2 (685)
            |- STATUS: db: unknown; conf: unknown; cond: unknown; dm: none; conn: unknown
            |- vdom:[3]root flags:0 adom:root pkg:[never-installed]
---End device list---
```

The example above shows device2 with an object ID of 125 and that of device1 is 164.



If the FortiAnalyzer device list is verified prior to upgrade to 5.2.6 and a slave device is present as shown above, it can be deleted using the steps as defined in the workaround section of this CSB. Once the device has been removed, the FortiAnalyzer can be upgraded to 5.2.6 without the risk of encountering this issue.

Possibly Affected Products:

FortiAnalyzer 5.2.6

Remedy:

FortiAnalyzer 5.2.7, estimated to be released between April 20 to 21, 2016.

Workaround:

You can restore logging functionality by deleting the slave units which have lower OID numbers and then rebooting the FortiAnalyzer. To delete the units, from GUI\Device Manager\<right click on the device>\delete.

Technical Support Contact Information:
http://www.fortinet.com/support/contact_support.html
Fortinet technical support home page: https://support.fortinet.com

All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Statements contained herein were attained in internal lab tests under ideal conditions, and performance may vary; network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment or admission of fault by Fortinet, and Fortinet disclaims all representations and warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet' s General Counsel, with an express representation or warranty included therein. All Fortinet end-customers are bound by the terms of Fortinet' s current End User License Agreement. The information in this Customer Support Bulletin is provided for remedial purposes and is designed to assist customers in corrective action that may be helpful to the customer.